Available online at www.sciencedirect.com

ScienceDirect

Discrete Applied Mathematics 155 (2007) 1224–1232

DISCRETE APPLIED MATHEMATICS

www.elsevier.com/locate/dam

Better upper bounds on the QOBDD size of integer multiplication

Kazuyuki Amano[a,*], Akira Maruoka[b]

[a] *Department of Computer Science, Gunma University, Tenjin 1-5-1, Kiryu, Gunma 376-8515, Japan*
[b] *Graduate School of Information Sciences, Tohoku University, Aoba 6-6-05, Aramaki, Sendai 980-8579, Japan*

Received 6 October 2005; received in revised form 16 November 2006; accepted 26 November 2006
Available online 18 January 2007

Abstract

We show that the middle bit of the multiplication of two n-bit integers can be computed by an ordered binary decision diagram (OBDD) of size less than $2.8 \cdot 2^{6n/5}$. This improves the previously known upper bound of $(\frac{7}{3}) \cdot 2^{4n/3}$ by Woelfel (New Bounds on the OBDD-size of integer multiplication via Universal Hashing, J. Comput. System Sci. 71(4) (2005) 520–534). The experimental results suggest that our exponent of $6n/5$ is optimal or at least very close to optimal. A general upper bound of $O(2^{3n/2})$ on the OBDD size of each output bit of the multiplication is also presented.

Keywords: Ordered binary decision diagram; Integer multiplication; Upper bounds

1. Introduction

Ordered binary decision diagrams (OBDDs), which were first introduced by Bryant [4], are nowadays one of the most well-established computational models for representing and manipulating Boolean functions. OBDDs are widely used in the areas of hardware verification, model checking, and computer aided design (see e.g. [9,13]).

Definition 1. Let $X_n = \{x_1, \ldots, x_n\}$ be a set of Boolean variables. A variable ordering π on X_n is a permutation from $\{1, \ldots, n\}$ to X_n leading to the ordered list $\pi(1), \ldots, \pi(n)$ of the variables.

A π-OBDD on X_n is a directed acyclic graph whose sinks are labeled by a constant 0 or 1 and whose inner nodes are labeled by Boolean variables from X_n. Each inner node has two outgoing edges, one of them labeled by 0, the other by 1. The edges between inner nodes have to respect the variable ordering π, i.e., if an edge leads from an x_i-nodes to an x_j-node, then $\pi^{-1}(x_i) < \pi^{-1}(x_j)$. Each node v represents a Boolean function $f_v : \{0,1\}^n \to \{0,1\}$ defined in the following way: an assignment $(a_1, \ldots, a_n) \in \{0,1\}^n$ to X_n defines a uniquely determined path from v to one of the sinks. The label of the reached sink gives $f_v(a)$. The size of a π-OBDD is defined as the number of its nodes. The OBDD size of f, denoted by $\mathrm{OBDD}(f)$ is the minimum size of all π-OBDDs that compute f. A π-OBDD for some unspecified variable order is simply called OBDD.

For many practically relevant functions, such as symmetric functions, the corresponding OBDD representations are quite small. However, for several important functions, exponential lower bounds on the size of an OBDD representation

* Corresponding author.
E-mail addresses: amano@cs.gunma-u.ac.jp (K. Amano), maruoka@ecei.tohoku.ac.jp (A. Maruoka).

0166-218X/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.dam.2006.11.010

are known. The integer multiplication is one of the most important such functions since it is hard to represent by OBDDs and is realized in hardware. By this reason, the OBDD size of integer multiplication has been of considerable interest.

Definition 2. For each $0 \leqslant k \leqslant 2n-1$, let $\mathsf{MUL}_{k,n} : \{0,1\}^{2n} \to \{0,1\}$ denote the Boolean function that outputs z_k of the product $(z_{2n-1} \cdots z_0)$ of two n-bit integers $(x_{n-1} \cdots x_0)$ and $(y_{n-1} \cdots y_0)$, where x_0, y_0 and z_0 are the least significant bits.

The middle bit of integer multiplication is denoted by $\mathsf{MUL}_{n-1,n}$. Since for any Boolean function on m variables, there exists an OBDD of size $(2+\varepsilon)2^m/m$ [8], the trivial upper bound on OBDD($\mathsf{MUL}_{n-1,n}$) is $O(2^{2n}/n)$. In 1991, Bryant [5] first proved an exponential lower bound of $2^{n/8}$ on OBDD($\mathsf{MUL}_{n-1,n}$). Only recently, Woelfel has succeeded to improve the upper and lower bounds on the size of OBDD for $\mathsf{MUL}_{n-1,n}$ [15]. Precisely, he showed that OBDD($\mathsf{MUL}_{n-1,n}$) is between $2^{n/2}/61$ and $(7/3) \cdot 2^{4n/3}$. His lower bound rules out the possibility of constructing an OBDD for 64-bit multiplication with a reasonable size. Nevertheless, there still exists a considerable gap between the upper and lower bounds. The complexity of multiplication for more general models than OBDDs has been extensively studied recently (e.g. [1,3,11,14]).

The main objective of this work is to determine the asymptotic behavior of the size of OBDDs for $\mathsf{MUL}_{n-1,n}$, or more generally, for $\mathsf{MUL}_{k,n}$. In the paper, we mainly consider a restricted variant of OBDDs which is called *leveled* OBDDs or *quasi*-OBDDs, denoted by QOBDDs. This is because analyzing the size of QOBDDs is easier than that of OBDDs.

Definition 3. A π-QOBDD is a π-OBDD with the additional property that each edge from a $\pi(i)$-node for $i < n$ reaches a $\pi(i+1)$-node. In other words, each path in a π-QOBDD examines every variable exactly once in the order determined by π. Let π-QOBDD(f) denote the minimum size of π-QOBDDs that compute f. The QOBDD size of a Boolean function f, denoted by QOBDD(f) is the minimum size of all π-QOBDDs that compute f, i.e., $\mathrm{QOBDD}(f) = \min_\pi \pi\text{-QOBDD}(f)$. A π-QOBDD for some unspecified variable order is simply called QOBDD.

Since every π-OBDD can be transformed into a π-QOBDD by inserting dummy nodes on paths from the root to a sink, it is obvious that

$$\mathrm{OBDD}(f) \leqslant \mathrm{QOBDD}(f) \leqslant (n+1)\mathrm{OBDD}(f)$$

for every Boolean function f on n variables. Thus, the size of QOBDDs can be considered essentially the same as that of OBDDs, especially for a function having an exponential complexity, such as multiplication. A detailed discussion on the relationship between the OBDD size and the QOBDD size can be found in e.g. [2,8].

The contributions of the paper are as follows: First, in Section 2, we show that $\mathsf{MUL}_{n-1,n}$ can be computed by a QOBDD of size less than $2.8 \cdot 2^{6n/5}$, which improves the previously known upper bound of $(\frac{7}{3}) \cdot 2^{4n/3}$ [15]. This is achieved essentially by finding a good variable ordering for $\mathsf{MUL}_{n-1,n}$. Second, we obtain the optimal QOBDDs for $\mathsf{MUL}_{n-1,n}$ for small values of n by an exhaustive search using a computer, and analyze them. Interestingly, our experimental results suggest that the exponent of $6n/5$ in our upper bound is the true exponent of the QOBDD size of $\mathsf{MUL}_{n-1,n}$. This will be described in Section 3. Next, in Section 4, we give a general upper bound on the QOBDD size of each output bit of integer multiplication. Precisely, we show that $\mathrm{QOBDD}(\mathsf{MUL}_{k,n}) = O(2^c)$ where $c = 6k/5$ for $0 \leqslant k \leqslant 5n/4$, $c = 3n/2$ for $5n/4 < k \leqslant 3n/2$, and $c = 3n-k$ for $3n/2 < k \leqslant 2n-1$. Finally, in Section 5, we describe some open problems for further research.

2. Upper bounds for $\mathsf{MUL}_{n-1,n}$

In this section, we show an upper bound of $2.8 \cdot 2^{6n/5}$ on the OBDD size of the middle bit of integer multiplication.

Let $X = (x_{n-1} \cdots x_0)$ be an n-bit binary string. We also use X to denote the integer represented by $x_{n-1} \cdots x_0$, i.e., $X = \sum_{i=0}^{n-1} 2^i x_i$. For $0 \leqslant i \leqslant j \leqslant n-1$, let $[X]_i^j$ be the integer represented by the substring $x_j \cdots x_i$. Formally,

$$[X]_i^j = (X \ \mathrm{div}\ 2^i) \ \mathrm{mod}\ 2^{j-i+1} = (X \ \mathrm{mod}\ 2^{j+1}) \ \mathrm{div}\ 2^i.$$

Here we use the operators "mod" that gives the integer reminder of division, and "div" that gives the integer result of division. We abbreviate $[X]_i^i$ by $[X]_i$. For a set S, $|S|$ denotes the cardinality of S.

Theorem 4. *There is a* QOBDD *for* $\mathsf{MUL}_{n-1,n}$ *whose size is less than* $2.8 \cdot 2^{6n/5}$.

Proof. Let $X = (x_{n-1} \cdots x_0)$ and $Y = (y_{n-1} \cdots y_0)$ be the input variables for $\mathsf{MUL}_{n-1,n}$. Let π be the variable ordering $(x_0, y_0, x_1, y_1, \ldots, x_{n-1}, y_{n-1})$. For the sake of simplicity, we suppose that n is a multiple of 5. (Other cases will be discussed later.) Below we show that π-QOBDD$(\mathsf{MUL}_{n-1,n}) \leqslant \frac{19}{7} \cdot 2^{6n/5} < 2.72 \cdot 2^{6n/5}$.

Let $n = 5k$. Let $\mathscr{F}_{i,j}$ denote the set of subfunctions of $\mathsf{MUL}_{n-1,n}$ that obtained by replacing the variables $x_0, \ldots, x_{i-1}$ and $y_0, \ldots, y_{j-1}$ with constants. It is easy to verify that

$$\pi\text{-QOBDD}(\mathsf{MUL}_{n-1,n}) = |\mathscr{F}_{0,0}| + |\mathscr{F}_{1,0}| + |\mathscr{F}_{1,1}| + \cdots + |\mathscr{F}_{n,n}|. \tag{1}$$

This is because that the number of x_i-nodes (y_i-nodes, resp.) in an optimal π-QOBDD for $\mathsf{MUL}_{n-1,n}$ is shown to be $|\mathscr{F}_{i,i}|$ ($|\mathscr{F}_{i+1,i}|$, resp.) [12, Theorem 1]. Thus, our goal is to bound the number of different subfunctions in $\mathscr{F}_{i,i}$ and in $\mathscr{F}_{i+1,i}$.

We first bound the size of $\mathscr{F}_{i,i}$. Suppose that $n/2 \leqslant i < n$.

Let $X_{\mathrm{L}} = (x_{i-1} \cdots x_0)$, $Y_{\mathrm{L}} = (y_{i-1} \cdots y_0)$, $X_{\mathrm{H}} = X \setminus X_{\mathrm{L}} = (x_{n-1} \cdots x_i)$ and $Y_{\mathrm{H}} = Y \setminus Y_{\mathrm{L}} = (y_{n-1} \cdots y_i)$, which means that $X = 2^i X_{\mathrm{H}} + X_{\mathrm{L}}$ and $Y = 2^i Y_{\mathrm{H}} + Y_{\mathrm{L}}$. We focus on the "middle part" of $X \cdot Y$, namely, $[X \cdot Y]_i^{n-1}$ of which the most significant bit represents $\mathsf{MUL}_{n-1,n}(X, Y)$. We have

$$\begin{aligned} X \cdot Y \mod 2^n &= (2^i X_{\mathrm{H}} + X_{\mathrm{L}}) \cdot (2^i Y_{\mathrm{H}} + Y_{\mathrm{L}}) \mod 2^n \\ &= \left(2^i (X_{\mathrm{H}} \cdot Y_{\mathrm{L}} + Y_{\mathrm{H}} \cdot X_{\mathrm{L}}) + X_{\mathrm{L}} \cdot Y_{\mathrm{L}}\right) \mod 2^n \\ &= (2^i (X_{\mathrm{H}} \cdot [Y_{\mathrm{L}}]_0^{n-i-1} + Y_{\mathrm{H}} \cdot [X_{\mathrm{L}}]_0^{n-i-1}) + [X_{\mathrm{L}} \cdot Y_{\mathrm{L}}]_0^{n-1}) \mod 2^n. \end{aligned}$$

Further, we have

$$\begin{aligned} [X \cdot Y]_i^{n-1} &= (X \cdot Y \mod 2^n) \operatorname{div} 2^i \\ &= (X_{\mathrm{H}} \cdot [Y_{\mathrm{L}}]_0^{n-i-1} + Y_{\mathrm{H}} \cdot [X_{\mathrm{L}}]_0^{n-i-1} + [X_{\mathrm{L}} \cdot Y_{\mathrm{L}}]_i^{n-1}) \mod 2^{n-i}. \end{aligned}$$

This implies that the value of $[X \cdot Y]_i^{n-1}$ and hence $\mathsf{MUL}_{n-1,n}(X, Y)$ is uniquely determined by X_{H}, Y_{H}, $[X_{\mathrm{L}}]_0^{n-i-1}$, $[Y_{\mathrm{L}}]_0^{n-i-1}$ and $[X_{\mathrm{L}} \cdot Y_{\mathrm{L}}]_i^{n-1}$. Hence, each subfunction $f_{X_{\mathrm{L}}, Y_{\mathrm{L}}} \in \mathscr{F}_{i,i}$ is uniquely determined by $[X_{\mathrm{L}}]_0^{n-i-1}$, $[Y_{\mathrm{L}}]_0^{n-i-1}$ and $[X_{\mathrm{L}} \cdot Y_{\mathrm{L}}]_i^{n-1}$, each of them has length $n-i$. Therefore, we have $|\mathscr{F}_{i,i}| \leqslant 2^{3(n-i)}$ for $n/2 \leqslant i < n$. Note that this bound is better than the trivial upper bound of $|\mathscr{F}_{i,i}| \leqslant 2^{2i}$ when $i > 3n/5$. By an analogous argument to the case of $|\mathscr{F}_{i,i}|$, we can also show that $|\mathscr{F}_{i+1,i}| \leqslant 2^{3(n-i)-1}$ for $n/2 \leqslant i < n$, which is better than the trivial bound of $|\mathscr{F}_{i+1,i}| \leqslant 2^{2i+1}$ for $i \geqslant 3n/5$.

The upper bound of π-QOBDD$(\mathsf{MUL}_{n-1,n})$ is now easily derived by plugging these bounds into Eq. (1). Namely, we have

$$\begin{aligned} \pi\text{-QOBDD}(\mathsf{MUL}_{n-1,n}) &= \sum_{i=0}^{3k-1} (|\mathscr{F}_{i,i}| + |\mathscr{F}_{i+1,i}|) + \sum_{i=3k}^{5k-1} (|\mathscr{F}_{i,i}| + |\mathscr{F}_{i+1,i}|) + |\mathscr{F}_{n,n}| \\ &\leqslant \sum_{i=0}^{6k-1} 2^i + \sum_{i=3k}^{5k-1} (2^{3(5k-i)} + 2^{3(5k-i)-1}) + 2 \\ &= 2^{6k} - 1 + \left(1 + \frac{1}{2}\right) \sum_{i=1}^{2k} 2^{3i} + 2 \\ &= 2^{6k} + \frac{3}{2} \cdot \frac{8(2^{6k} - 1)}{7} + 1 < \frac{19}{7} \cdot 2^{6k}, \end{aligned}$$

which completes the proof for the case $n = 5k$.

The other cases, i.e., $n = 5k + \alpha$ for $\alpha \in \{1, 2, 3, 4\}$, can be shown analogously. The upper bounds are $\frac{40}{7} \cdot 2^{6k}$, $\frac{96}{7} \cdot 2^{6k}$, $\frac{208}{7} \cdot 2^{6k}$ and $\frac{544}{7} \cdot 2^{6k}$ for $\alpha = 1, 2, 3$ and 4, respectively. By a simple case checking, we can see that all these values are bounded by $2.8 \cdot 2^{6n/5}$. Note that the largest constant $(= (\frac{544}{7})/2^{4.8} \sim 2.7897)$ is attained when $\alpha = 4$. □

Remark that we use the variable ordering $\pi=(x_0, y_0, \ldots, x_{n-1}, y_{n-1})$ in the proof of Theorem 4, whereas Woelfel [15] used the ordering $\pi=(x_0, \ldots, x_{n-1}, y_0, \ldots, y_{n-1})$ to show the upper bound of $O(2^{4n/3})$. Remarkably, the experimental results suggest that the exponent of $6n/5$ in Theorem 4 is (at least very close to) the true exponent of the QOBDD size of $\mathsf{MUL}_{n-1,n}$, which we will describe in the next section.

3. Experimental results

In this section, we describe the experimental results supporting the conjecture that the exponent of $6n/5$ in the upper bound in Theorem 4 is optimal.

We did an exhaustive search by using a computer to find the optimal QOBDDs for $\mathsf{MUL}_{n-1,n}$ for small values of n. Throughout our experiments, we consider QOBDDs instead of OBDDs. This is because a good estimation of the number of subfunctions obtained by fixing variables appropriately seems to be crucial to obtain good upper and lower bounds on the OBDD size of $\mathsf{MUL}_{n-1,n}$. We believe that in order to analyze such numbers it is better to consider the size of QOBDDs than that of OBDDs since there is a strong connection between the number of subfunctions and size of an optimal QOBDD (see Eq. (1)). Note that the best known algorithm for computing an optimal OBDD for a given function has an exponential running time [6,7]. We believe that computing an optimal QOBDD is almost as hard as computing an optimal OBDD.

We use a standard dynamic programming approach to compute the size of optimal QOBDDs for $\mathsf{MUL}_{n-1,n}$ which we briefly describe below.

Let f be a Boolean function over the set of variables $X=\{x_1, \ldots, x_n\}$. For $I \subseteq X$, let $\mathrm{sub}(f, I)$ denote the number of subfunctions of f which we obtain by fixing all variables in $X\backslash I$ to constants. Since the number of $\pi(i)$-nodes in an optimal π-QOBDD for f is equal to $\mathrm{sub}(f, I)$ with $I=\{\pi(i+1), \ldots, \pi(n)\}$ [12], it is easy to verify that

$$\mathrm{QOBDD}(f) = \min_{\mathscr{I}=\{I_0,\ldots,I_n\}} \sum_{0 \leqslant i \leqslant n} \mathrm{sub}(f, I_i),$$

where the minimum ranges over all sequences of sets $\emptyset = I_0 \subset I_1 \subset \cdots \subset I_n = X$ with $|I_i| = i$. If we define $\mathrm{QOBDD}(f, I)$ for $I \subseteq X$ by the following recursion:

$$\mathrm{QOBDD}(f, I) = \min_{x \in I} \{\mathrm{QOBDD}(f, I\backslash\{x\}) + \mathrm{sub}(f, I)\}, \tag{2}$$

then $\mathrm{QOBDD}(f)$ is given by $\mathrm{QOBDD}(f, X)$. It should be noted that if we replace the term $\mathrm{sub}(f, I)$ in Eq. (2) by $\mathrm{sub}_x(f, I)$, which denotes the number of subfunctions of f obtained by fixing all variables in $X\backslash I$ that essentially depend on x, then we can obtain $\mathrm{OBDD}(f)$ in a similar fashion [6,7].

Using the above algorithm, we compute the size of optimal QOBDDs for $\mathsf{MUL}_{n-1,n}$ for $n \leqslant 12$. In addition, we also compute the minimum size of π-QOBDDs for $\mathsf{MUL}_{n-1,n}$ with the variable ordering $\pi=(x_0, y_0, x_1, y_1, \ldots, x_{n-1}, y_{n-1})$, which is used in the proof of Theorem 4.

The results are shown in Table 1. Remarkably, Table 1 shows that the QOBDD size of $\mathsf{MUL}_{n-1,n}$ and also the minimum size of π-QOBDDs for $\mathsf{MUL}_{n-1,n}$ are almost proportional to $2^{6n/5}$. This leads to a conjecture that $\mathrm{QOBDD}(\mathsf{MUL}_{n-1,n}) = \Theta(2^{6n/5})$, which means that the upper bound in Theorem 4 is tight up to a constant factor. Table 1 also shows that the optimal QOBDDs for $\mathsf{MUL}_{n-1,n}$ are almost 30% smaller than the optimal π-QOBDDs.

During the experiments, the optimal variable orderings for $\mathsf{MUL}_{n-1,n}$ are also obtained. For example, the optimal variable orderings for $\mathsf{MUL}_{n-1,n}$ for $n=8, \ldots, 12$ are

$(x_1, x_2, x_3, x_4, y_3, y_4, y_2, x_5, y_5, y_1, x_6, y_6, x_0, y_7, x_7, y_0)$,

$(x_1, x_2, x_3, x_4, y_4, x_5, y_3, y_5, y_2, y_1, x_6, y_6, x_7, y_7, x_0, y_8, x_8, y_0)$,

$(x_3, x_4, x_5, x_6, y_3, y_4, y_5, y_6, x_2, y_2, x_1, y_1, x_7, y_7, x_8, y_8, x_0, y_9, x_9, y_0)$,

$(x_3, x_4, x_5, x_6, x_7, y_4, y_5, y_6, y_7, y_3, x_2, y_2, x_1, y_1, x_8, y_8, x_9, y_9, x_0, y_{10}, x_{10}, y_0)$,

$(x_2, x_3, x_4, x_5, x_6, x_7, y_4, y_5, y_6, y_7, y_3, y_2, x_1, y_1, x_8, y_8, x_9, y_9, x_{10}, y_{10}, x_0, y_{11}, x_{11}, y_0)$.

We remark that the optimal variable ordering is not unique in general. We can see that, for all optimal orderings shown above, the last four variables are $x_0, y_{n-1}, x_{n-1}, y_0$. Motivated by this observation, we compute the size of π'-QOBDDs for $\mathsf{MUL}_{n-1,n}$ with the ordering $\pi'=(x_1, y_1, \ldots, x_{n-2}, y_{n-2}, x_0, y_{n-1}, x_{n-1}, y_0)$. The sizes of π'-QOBDD

Table 1
The QOBDD size of $\mathsf{MUL}_{n-1,n}$ is shown in the first column, and the minimum size of π-QOBDDs for $\mathsf{MUL}_{n-1,n}$ with the variable ordering $\pi = (x_0, y_0, \ldots, x_{n-1}, y_{n-1})$ is shown in the third column

n	QOBDD	QOBDD$/2^{6n/5}$	π-QOBDD	π-QOBDD$/2^{6n/5}$
4	39	1.40	56	2.01
5	72	1.13	109	1.70
6	156	1.06	230	1.56
7	348	1.03	490	1.45
8	797	1.03	1106	1.43
9	1808	1.01	2490	1.40
10	4106	1.00	5751	1.40
11	9796	1.04	13,228	1.41
12	22,151	1.02	30,862	1.43
13			71,239	1.43
14			166,981	1.46
15			384,586	1.47
16			892,007	1.48

for $\mathsf{MUL}_{n-1,n}$ for $n = 8, \ldots, 12$ are 824, 1853, 4280, 9945 and 22 744, respectively. Surprisingly, these are very close (within about 4%) to the optimal sizes shown in Table 1. By using the ordering π' instead of π in the proof of Theorem 4, we may have an upper bound with a slightly better constant factor than Theorem 4.

4. General upper bounds

In this section, we consider the size of a smallest QOBDD for the kth bit of integer multiplication for general values of k.

The problem of determining the hardest bit of the multiplication and its complexity is interesting and important since the total complexity of the multiplication may essentially depend on the complexity of the hardest bit. It is well known that the middle bit is the "hardest" bit, in the sense that if it can be computed by OBDDs of size $s(n)$, then any other bit can be computed with size at most $s(2n)$ (e.g. [10]). However, this does not assert that the middle bit is *exactly* the hardest bit. The experimental results suggest that the hardest bit is located higher than the middle. For example, for an 8 bit multiplication, we verified that the 10th output bit is the hardest for QOBDDs, namely, $\mathrm{QOBDD}(\mathsf{MUL}_{k,8}) = 797, 1623, 1937, 2041, 1755, 1175$ for $k = 7, 8, \ldots, 12$, respectively. Recall that the 0th bit is the least significant bit.

As was shown by Bryant [5], computing $\mathsf{MUL}_{k,n}$ is not harder than computing $\mathsf{MUL}_{k,k+1}$ for every k. Hence, the following corollary is a direct consequence of Theorem 4.

Corollary 5. *For every k, there exists a QOBDD for $\mathsf{MUL}_{k,n}$ whose size is $\mathrm{O}(2^{6k/5})$.*

Apparently, the upper bound in the above corollary overestimates the actual size of a smallest QOBDD for $\mathsf{MUL}_{k,n}$ if k is close to $2n$. The following theorem asserts that the OBDD size of every single bit of multiplication is bounded by $\mathrm{O}(2^{3n/2})$.

Theorem 6. *For every k, there exists a QOBDD for $\mathsf{MUL}_{k,n}$ whose size is $\mathrm{O}(2^{3n/2})$.*

For $a \in \{0, \ldots, 2^n - 1\}$, let $\mathsf{MUL}^a_{k,n} : \{0,1\}^n \to \{0,1\}$ be the function that outputs the kth bit of the product of a with an n-bit number, i.e., $\mathsf{MUL}^a_{k,n}(X) = \mathsf{MUL}_{k,n}(a, X)$. Here the 0th bit is the least significant bit. To prove the theorem, we use the following lemma, which is a generalization of the results of Woelfel [15, Theorem 13]. He showed that $\pi\text{-QOBDD}(\mathsf{MUL}^a_{k,n}) = \mathrm{O}(2^{n/2})$ for $k = n - 1$, when π is the variable ordering $(x_0, x_1, \ldots, x_{n-1})$.

Lemma 7. *Let $Y = (y_{n-1} \cdots y_0)$ be an n-bit integer and let π be the variable ordering $(y_0, y_1, \ldots, y_{n-1})$. Then for every $k \geqslant n$ and for every $a \in \{0, \ldots, 2^n - 1\}$, the π-QOBDD size for computing $\mathsf{MUL}^a_{k,n}(Y)$ is $\mathrm{O}(2^{n/2})$.*

Proof. Let $\mathscr{F}_i$ be the set of subfunctions of $\mathsf{MUL}^a_{k,n}$ which we obtain by fixing the variables $y_0, \ldots, y_{i-1}$ to constants. We will upper bound the number of subfunctions in $\mathscr{F}_i$. Let $Y_{\mathrm{L}} = (y_{i-1} \cdots y_0)$ and $Y_{\mathrm{H}} = (y_{n-1} \cdots y_i)$. Note that

$$\mathsf{MUL}^a_{k,n}(Y) = \mathsf{MUL}^a_{k,n}(Y_{\mathrm{H}} \circ Y_{\mathrm{L}}) = ((aY_{\mathrm{H}}2^i + aY_{\mathrm{L}}) \mod 2^{k+1}) \operatorname{div} 2^k.$$

Here and hereafter, for an i-bit integer ℓ and an $(n-i)$-bit integer h, $h \circ \ell$ denotes the n-bit integer $2^i h + \ell$.

For $h \in \{0, \ldots, 2^{n-i}-1\}$, let $z_h = ah2^i \mod 2^{k+1}$. Let $\rho : \{0, \ldots, 2^{n-i}-1\} \to \{0, \ldots, 2^{n-i}-1\}$ be a permutation such that the $(i+1)$th smallest of $z_0, \ldots, z_{2^{n-i}-1}$ is equal to $z_{\rho(i)}$. (The tie is broken arbitrary. In fact, we only need the condition that $0 \leqslant z_{\rho(0)} \leqslant z_{\rho(1)} \leqslant \cdots \leqslant z_{\rho(2^{n-i}-1)} < 2^k$.) For the sake of simplicity, we denote that $z_{\rho(-1)} = 0$ and $z_{\rho(2^{n-i})} = 2^k$.

We now claim that for every two distinct integers $\ell, \ell' \in \{0, \ldots, 2^i - 1\}$ such that

$$\begin{cases} z_{\rho(t-1)} < 2^k - (a\ell \mod 2^{k+1}) \leqslant z_{\rho(t)}, \\ z_{\rho(t-1)} < 2^k - (a\ell' \mod 2^{k+1}) \leqslant z_{\rho(t)}, \end{cases} \tag{3}$$

or

$$\begin{cases} z_{\rho(t-1)} < 2^{k+1} - (a\ell \mod 2^{k+1}) \leqslant z_{\rho(t)}, \\ z_{\rho(t-1)} < 2^{k+1} - (a\ell' \mod 2^{k+1}) \leqslant z_{\rho(t)}, \end{cases} \tag{4}$$

for some $0 \leqslant t \leqslant 2^{n-i}$, the subfunctions of $\mathsf{MUL}^a_{k,n}$ obtained by fixing Y_L to ℓ and to ℓ' are identical. In other words, if $2^k - (a\ell \mod 2^{k+1})$ and $2^k - (a\ell' \mod 2^{k+1})$, or $2^{k+1} - (a\ell \mod 2^{k+1})$ and $2^{k+1} - (a\ell' \mod 2^{k+1})$ lie in a same "interval", then two functions $\mathsf{MUL}^a_{k,n}(Y_{\mathrm{H}} \circ \ell)$ and $\mathsf{MUL}^a_{k,n}(Y_{\mathrm{H}} \circ \ell')$ (on Y_{H}) are identical.

The claim is proved as follows. We assume that ℓ and ℓ' satisfy condition (3). (The proof for the case (4) is analogous to this case.) Since $0 \leqslant z_{\rho(t-1)} + a\ell \mod 2^{k+1} < 2^k$ and $0 \leqslant z_{\rho(t-1)} + a\ell' \mod 2^{k+1} < 2^k$, we have that $\mathsf{MUL}^a_{k,n}(h \circ \ell) = \mathsf{MUL}^a_{k,n}(h \circ \ell')$ for every $h = \rho(t')$ with $t' \in \{0, 1, \ldots, t-1\}$. Similarly, since $2^k \leqslant z_{\rho(t)} + a\ell \mod 2^{k+1} < 2^{k+1}$ and $2^k \leqslant z_{\rho(t)} + a\ell' \mod 2^{k+1} < 2^{k+1}$, we have that $\mathsf{MUL}^a_{k,n}(h \circ \ell) = \mathsf{MUL}^a_{k,n}(h \circ \ell')$ for every $h = \rho(t')$ with $t' \in \{t, \ldots, 2^{n-i}-1\}$. Hence, we can conclude that $\mathsf{MUL}^a_{k,n}(h \circ \ell) = \mathsf{MUL}^a_{k,n}(h \circ \ell')$ for every $h \in \{0, \ldots, 2^{n-i}-1\}$, completing the proof of the claim.

The claim immediately implies that the number of subfunctions in $\mathscr{F}_i$ is bounded by the number of such intervals. This number is at most $2(2^{n-i}+1)$ since there are $2^{n-i}+1$ choices of t and for each t, there are two intervals corresponding to the cases (3) and (4). This gives a better upper bound on $|\mathscr{F}_i|$ than the trivial upper bound of 2^i when $i > (n+1)/2$. Hence, the size of a π-QOBDD is bounded by

$$\pi\text{-QOBDD}(\mathsf{MUL}^a_{k,n}) = \sum_{i=0}^{n} |\mathscr{F}_i| = \sum_{0 \leqslant i \leqslant \lceil n/2 \rceil} 2^i + \sum_{\lceil n/2 \rceil < i \leqslant n} 2(2^{n-i}+1) = \mathrm{O}(2^{n/2}).$$

This completes the proof of Lemma 7. □

Theorem 6 follows immediately from Lemma 7.

Proof of Theorem 6. Let $X = (x_{n-1} \cdots x_0)$ and $Y = (y_{n-1} \cdots y_0)$ be the input variables for $\mathsf{MUL}_{k,n}$. We first construct a full binary tree T of depth n which examines all the variables in X. Note that each leaf in T corresponds to an n-bit integer. Then, for each leaf in T that corresponds to an integer a, we connect a π-QOBDD that computes $\mathsf{MUL}^a_{k,n}(Y)$ to the leaf where π is the ordering with $\pi(i) = y_{i-1}$ for every i. Lemma 7 guarantees that the resulting QOBDD computes $\mathsf{MUL}_{k,n}$ and whose size is $\mathrm{O}(2^n 2^{n/2}) = \mathrm{O}(2^{3n/2})$. □

As one might expect, if the value of k is large enough, then a better upper bound can be obtained.

Theorem 8. *For every $k \geqslant n$, there exists a QOBDD for $\mathsf{MUL}_{k,n}$ whose size is $\mathrm{O}(2^{3n-k})$.*

Proof. Let $X = (x_{n-1} \cdots x_0)$ and $Y = (y_{n-1} \cdots y_0)$ be the input variables for $\mathsf{MUL}_{k,n}$. Let π be the variable ordering $(x_{n-1}, y_{n-1}, x_{n-2}, y_{n-2}, \ldots, x_0, y_0)$. Let $\mathscr{F}_{i,j}$ denote the set of subfunctions of $\mathsf{MUL}_{k,n}$ that obtained by fixing the

variables $x_{n-1}, \ldots, x_{n-i}$ and $y_{n-1}, \ldots, y_{n-j}$ to constants. Note that the suffixes i and j indicate the number of fixed variables in X and Y, respectively.

In the following, we bound the number of subfunctions in $\mathscr{F}_{i,i}$. Let $X_{\mathrm{H}} = (x_{n-1} \cdots x_{n-i})$, $Y_{\mathrm{H}} = (y_{n-1} \cdots y_{n-i})$, $X_{\mathrm{L}} = (x_{n-i-1} \cdots x_0)$ and $Y_{\mathrm{L}} = (y_{n-i-1} \cdots y_0)$, or equivalently, $X = 2^{n-i}X_{\mathrm{H}} + X_{\mathrm{L}}$ and $Y = 2^{n-i}Y_{\mathrm{H}} + Y_{\mathrm{L}}$. We obtain

$$\begin{aligned} & X \cdot Y \mod 2^{k+1} \\ &= \left((2^{n-i}X_{\mathrm{H}} + X_{\mathrm{L}}) \cdot (2^{n-i}Y_{\mathrm{H}} + Y_{\mathrm{L}})\right) \mod 2^{k+1} \\ &= \left(2^{2(n-i)}X_{\mathrm{H}} \cdot Y_{\mathrm{H}} + 2^{n-i}(X_{\mathrm{H}} \cdot Y_{\mathrm{L}} + X_{\mathrm{L}} \cdot Y_{\mathrm{H}}) + X_{\mathrm{L}} \cdot Y_{\mathrm{L}}\right) \mod 2^{k+1}. \end{aligned} \tag{5}$$

Suppose that $k \geqslant 2n-i+3$. (We will use the trivial upper bounds of $|\mathscr{F}_{i,i}| \leqslant 2^{2i}$ for the other case, i.e., for $i < 2n-k+3$.) Let $l = k - (2n-i) + 1$. For a pair of integers $(X_{\mathrm{H}}, Y_{\mathrm{H}})$, let Z_{H} and Z_{L} be two integers, depending on $(X_{\mathrm{H}}, Y_{\mathrm{H}})$, such that

$$(2^{2(n-i)}X_{\mathrm{H}} \cdot Y_{\mathrm{H}}) \mod 2^{k+1} = 2^{2n-i}Z_{\mathrm{H}} + Z_{\mathrm{L}}, \tag{6}$$

where $0 \leqslant Z_{\mathrm{H}} < 2^l$ and $0 \leqslant Z_{\mathrm{L}} < 2^{2n-i}$. In other words, Z_{H} and Z_{L} are the high l bits and the low $(2n-i)$ bits of the LHS of Eq. (6), respectively. From Eqs. (5) and (6), $\mathrm{MUL}_{k,n}(X, Y)$ is given by the most significant bit of

$$(2^{2n-i}Z_{\mathrm{H}} + Z_{\mathrm{L}} + 2^{n-i}(X_{\mathrm{H}} \cdot Y_{\mathrm{L}} + X_{\mathrm{L}} \cdot Y_{\mathrm{H}}) + X_{\mathrm{L}} \cdot Y_{\mathrm{L}}) \mod 2^{k+1}. \tag{7}$$

Since

$$Z_{\mathrm{L}} + 2^{n-i}(X_{\mathrm{H}} \cdot Y_{\mathrm{L}} + X_{\mathrm{L}} \cdot Y_{\mathrm{H}}) + X_{\mathrm{L}} \cdot Y_{\mathrm{L}} < 3 \cdot 2^{2n-i}, \tag{8}$$

if the jth bit of the binary representation of Z_{H} is 0 for some $j \geqslant 2$, then the most significant bit of Eq. (7) is equal to the most significant bit of $(2^{2n-i}Z_{\mathrm{H}} \mod 2^{k+1})$. Hence, for every pairs of integers $(X_{\mathrm{H}}, Y_{\mathrm{H}})$ that satisfies $[Z_{\mathrm{H}}]_j = 0$ for some $j \geqslant 2$, the subfunction of $\mathsf{MUL}_{k,n}$ obtained by fixing the high i bits of X to X_{H} and the high i bits of Y to Y_{H} is a constant function. Therefore, the number of subfunctions in $\mathscr{F}_{i,i}$ is bounded by 2 plus the number of pairs of integers $(X_{\mathrm{H}}, Y_{\mathrm{H}})$ that satisfy the condition that $[Z_{\mathrm{H}}]_j = 1$ for every $2 \leqslant j \leqslant l-2$, or equivalently the product $X_{\mathrm{H}} \cdot Y_{\mathrm{H}}$ is in the interval from $(a2^{i+l-1} - 2^{i+2})$ to $(a2^{i+l-1} - 1)$ for some integer $a \geqslant 1$.

If $2^i Y_{\mathrm{H}} \leqslant 2^{i+l-1} - 2^{i+2}$, which is satisfied if $Y_{\mathrm{H}} \leqslant 2^{l-2}$, there are no pairs $(X_{\mathrm{H}}, Y_{\mathrm{H}})$ satisfying the above condition. If not, for every fixed $Y_{\mathrm{H}} > 2^{l-2}$, it is sufficient to consider an interval with $a \leqslant \lceil Y_{\mathrm{H}}2^i/2^{i+l-1} \rceil$ and the number of pairs $(X_{\mathrm{H}}, Y_{\mathrm{H}})$ contained in each interval is at most $\lceil 2^{i+2}/Y_{\mathrm{H}} \rceil$.

Hence the number of pairs satisfying the above condition is at most

$$\begin{aligned} \sum_{2^{l-2} < y < 2^i} \left\lceil \frac{2^{i+2}}{y} \right\rceil \left\lceil \frac{y2^i}{2^{i+l-1}} \right\rceil &\leqslant \sum_{2^{l-2} < y < 2^i} 2\frac{2^{i+2}}{y} \cdot 2\frac{y2^i}{2^{i+l-1}} \\ &= \sum_{2^{l-2} < y < 2^i} 2^{i-l+5} < 2^{2i-l+5}, \end{aligned}$$

where the first inequality follows from $\lceil y2^i/2^{i+l-1} \rceil \leqslant 2(y2^i/2^{i+l-1})$ when $y \geqslant 2^{l-2}$. Hence, we have

$$|\mathscr{F}_{i,i}| \leqslant 2 + 2^{2i-l+5} < 2^{2i-k+(2n-i)+5} = 2^{2n-k+i+5}, \tag{9}$$

which is better than the trivial bound of $|\mathscr{F}_{i,i}| \leqslant 2^{2i}$ when $i > 2n-k+5$. The total size of π-QOBDD for $\mathsf{MUL}_{k,n}$ is given by

$$\begin{aligned} \pi\text{-QOBDD}(\mathsf{MUL}_{k,n}) &= \sum_{0 \leqslant i < n} (|\mathscr{F}_{i,i}| + |\mathscr{F}_{i+1,i}|) + |\mathscr{F}_{n,n}| \\ &\leqslant 3 \sum_{0 \leqslant i < n} |\mathscr{F}_{i,i}| + 2. \end{aligned} \tag{10}$$

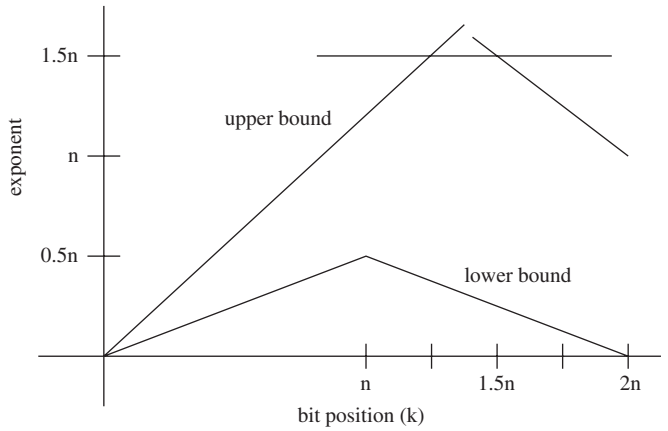

Fig. 1. The best known upper and lower bounds for the exponent of OBDD size for $\mathsf{MUL}_{k,n}$. The lower bound is by Woelfel [15]. The upper bound consists of three lines corresponding to three intervals in Theorem 9.

The last inequality follows from the simple fact that $|\mathscr{F}_{i+1,i}| \leqslant 2|\mathscr{F}_{i,i}|$ for every i. By plugging Eq. (9) into Eq. (10), we have

$$\pi\text{-QOBDD}(\mathsf{MUL}_{k,n}) \leqslant 3\left(\sum_{0\leqslant i\leqslant 2n-k+5} 2^{2i} + \sum_{2n-k+6\leqslant i<n} 2^{2n-k+i+5}\right) + 2$$
$$\leqslant 3(2^{4n-2k+11} + 2^{3n-k+6}) + 2 = \mathrm{O}(2^{3n-k}).$$

The last equality follows from the assumption that $k \geqslant n$. □

Combining Corollary 5, Theorems 6 and 8, we have the following corollary.

Corollary 9. *The QOBDD size of* $\mathsf{MUL}_{k,n}$ *is* $\mathrm{O}(2^c)$ *where*

$$c = \begin{cases} 6k/5 & \text{for } 0 \leqslant k \leqslant 5n/4, \\ 3n/2 & \text{for } 5n/4 < k \leqslant 3n/2, \\ 3n-k & \text{for } 3n/2 < k \leqslant 2n-1. \end{cases}$$

The theorem says that every single bit of the multiplication of two n-bit integers can be computed by a QOBDD (and also by an OBDD) of size $\mathrm{O}(2^{3n/2})$. Note that the best known lower bound for $\mathsf{MUL}_{k,n}$ is $2^{\lfloor (k+1)/2 \rfloor}/61$ for $k < n$ and $2^{\lfloor (2n-k-1)/2 \rfloor}/61$ for $k \geqslant n$ by Woelfel [15]. Fig. 1 shows the best known upper and lower bounds on the exponent of the OBDD size for the kth bit of multiplication. There are still considerable gaps between the upper and lower bounds.

5. Concluding remarks

In the paper, we improve the upper bound on the OBDD size of $\mathsf{MUL}_{n-1,n}$ to $2.8 \cdot 2^{6n/5}$, and give the experimental results that suggest that our upper bound $\Theta(2^{6n/5})$ is the true OBDD size of $\mathsf{MUL}_{n-1,n}$. Apparently, an important open problem is to improve the lower bound. The problem to determine the hardest bit of integer multiplication for OBDDs is also interesting. This is because the total OBDD size of multiplication is essentially depending on the OBDD size of the hardest bit of multiplication, and obtaining higher lower bounds may be easier for the hardest bit than for the middle bit.

Acknowledgments

The first author would like to thank Philipp Woelfel for answering my questions quickly and clearly. Both authors would like to thank anonymous referees for a large number of helpful comments and suggestions. This work was

partially supported by Grant-in-Aid for Scientific Research on Priority Areas "New Horizons in Computing" from MEXT of Japan.

References

[1] F. Ablayev, M. Karpinski, A lower bound for integer multiplication on randomized ordered read-once branching programs, Inform. and Comput. 186 (2003) 78–89.
[2] B. Bollig, I. Wegener, Asymptotically optimal lower bounds for OBDDs and the solution of some basic OBDD problems, J. Comput. System Sci. 61 (2000) 558–579.
[3] B. Bollig, P. Woelfel, Read-once branching program lower bound of $\Omega(2^{n/4})$ for integer multiplication using universal hashing, in: Proceedings of the 33rd STOC, 2001, pp. 419–424.
[4] R.E. Bryant, Graph-based algorithms for Boolean function manipulation, IEEE Trans. Comput. 35 (1986) 677–691.
[5] R.E. Bryant, On the complexity of VLSI implementations and graph representations of Boolean functions with applications to integer multiplication, IEEE Trans. Comput. 40 (1991) 205–213.
[6] S.J. Friedman, K.J. Supowit, Finding the optimal variable ordering for binary decision diagrams, IEEE Trans. Comput. 39 (1990) 710–713.
[7] N. Ishiura, H. Sawada, S. Yajima, Minimization of binary decision diagrams based on the exchanges of variables, in: Proceedings of the IEEE International Conference on Computer-Aided Design, 1991, pp. 472–475.
[8] H.T. Liaw, C.S. Lin, On the OBDD-representation of general Boolean functions, IEEE Trans. Comput. 41 (6) (1992) 661–664.
[9] C. Meinel, T. Theobald, Algorithms and Data Structures in VLSI Design—OBDD Foundations and Applications, Springer, Berlin, 1998.
[10] S. Ponzio, A lower bound for integer multiplication with read-once branching programs, SIAM J. Comput. 28 (3) (1998) 798–815.
[11] M. Sauerhoff, P. Woelfel, Time-space tradeoff lower bounds for integer multiplication and graphs of arithmetic functions, in: Proceedings of the 35th STOC, 2003, pp. 186–194.
[12] I. Wegener, The size of reduced OBDD's and optimal read-once branching programs, IEEE Trans. Comput. 43 (11) (1994) 1262–1269.
[13] I. Wegener, BDDs—design, analysis, complexity, and applications, Discrete Appl. Math. 138 (2004) 229–251.
[14] I. Wegener, P. Woelfel, New results on the complexity of the middle bit of multiplication, in: Proceedings of the 20th Conference on Computational Complexity, 2005, pp. 100–110.
[15] P. Woelfel, New bounds on the OBDD-size of integer multiplication via universal hashing, J. Comput. System Sci. 71 (4) (2005) 520–534.